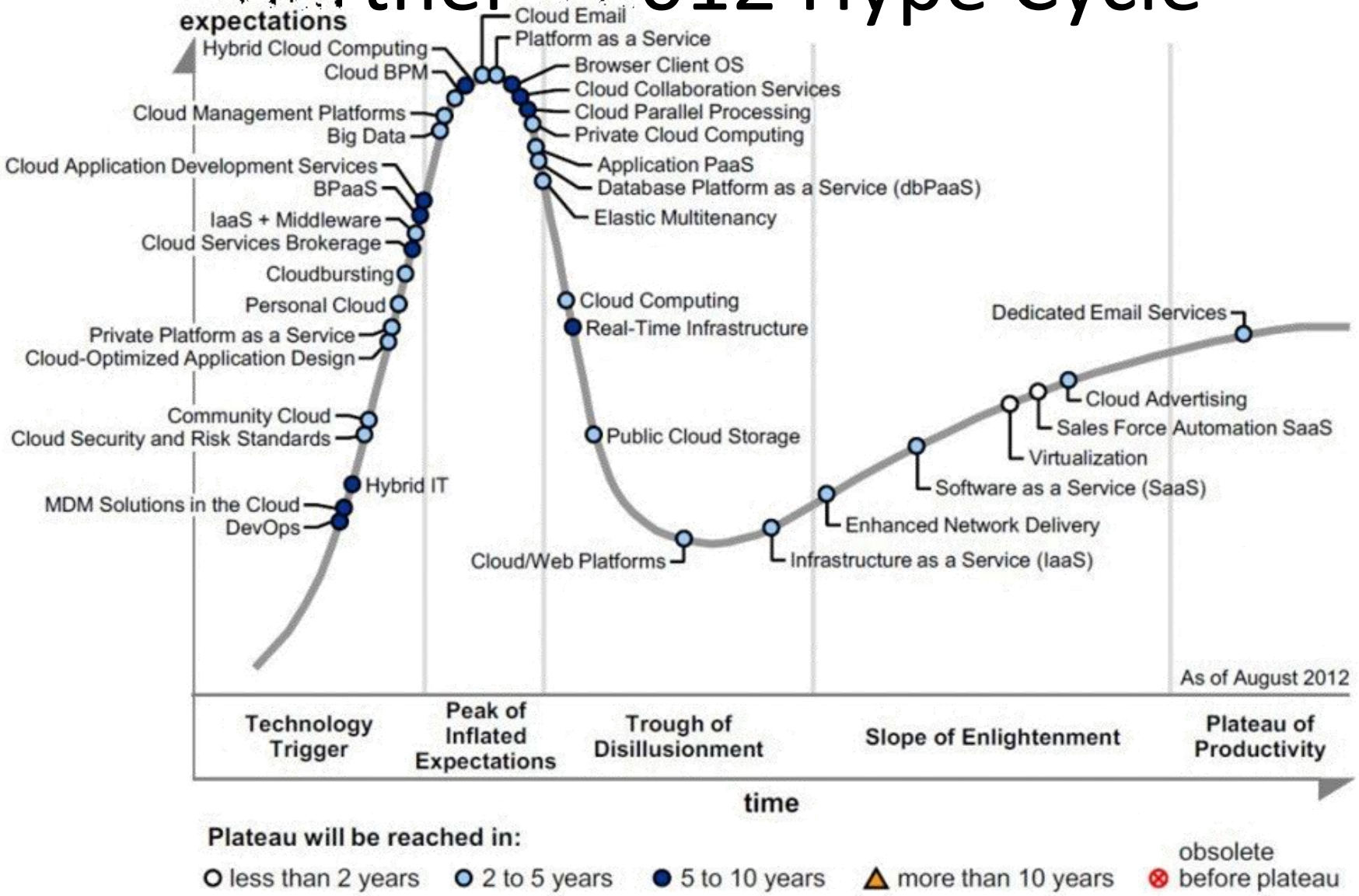
Tomorrow's Cloud

Security Concerns in a Broader Use of Clouds

Roy Campbell

University of Illinois at Urbana-Champaign

Gartner's 2012 Hype Cycle



Innovative Use of Advances in Computing

Cloud computing infrastructure

Robust computing at low-cost , "pay-as-you-go"

Assuring security and safety of the nation

United States Air Force global vigilance, reach and power

Smarter Planet Ecosystem Solutions which are:

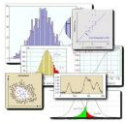
- **Cost effective**
- **Environment friendly**
- **Trustworthy**

Large volume of data

Phones, Sensors

Smart cars

Analysis



Integration

HMI

Individuals & enterprises

Human expertise
Innovations
Education
Research

Benefits to individuals & society

Modern health care
Adaptive Power Grid
Efficient transportation (air, ground, sea)
Preservation of water
New age agriculture

References

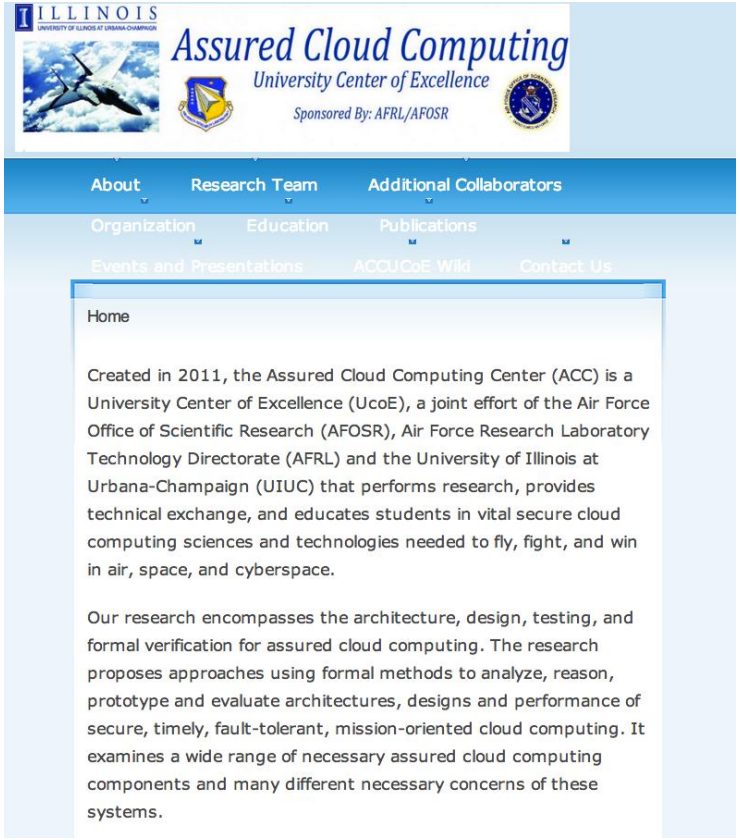
Report to the National Science Foundation
Directorate for Computer and Information Science and Engineering (CISE)

Security for Cloud Computing

Klara Nahrstedt and Roy Campbell
University of Illinois at Urbana-Champaign

March 15-16, 2012
Arlington, Virginia

http://illinois.edu/blog/view/695/66281?count=1&ACTION=DIALOG

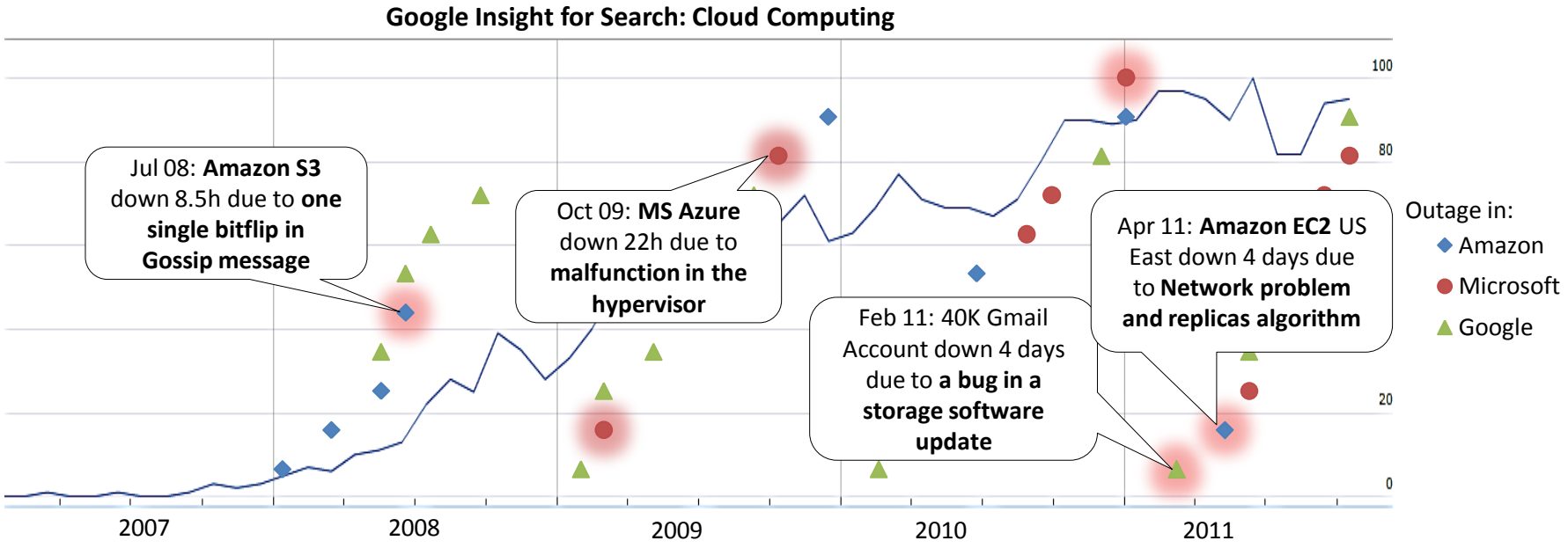


https://illinois.edu/blog/dialogFileSec/2737.pdf http://assured-cloud-computing.illinois.edu/

Outline

- Principles
- Security at scale
  - Adversary models for cloud computing
  - Management and monitoring
  - End-to-end security in cloud computing
  - Privacy of user and data
  - Delegation and authorization in cloud computing
- Dependability at scale
  - Characterizing failures in big-data systems
  - Managing metadata
  - Cloud, machine learning, and dependability

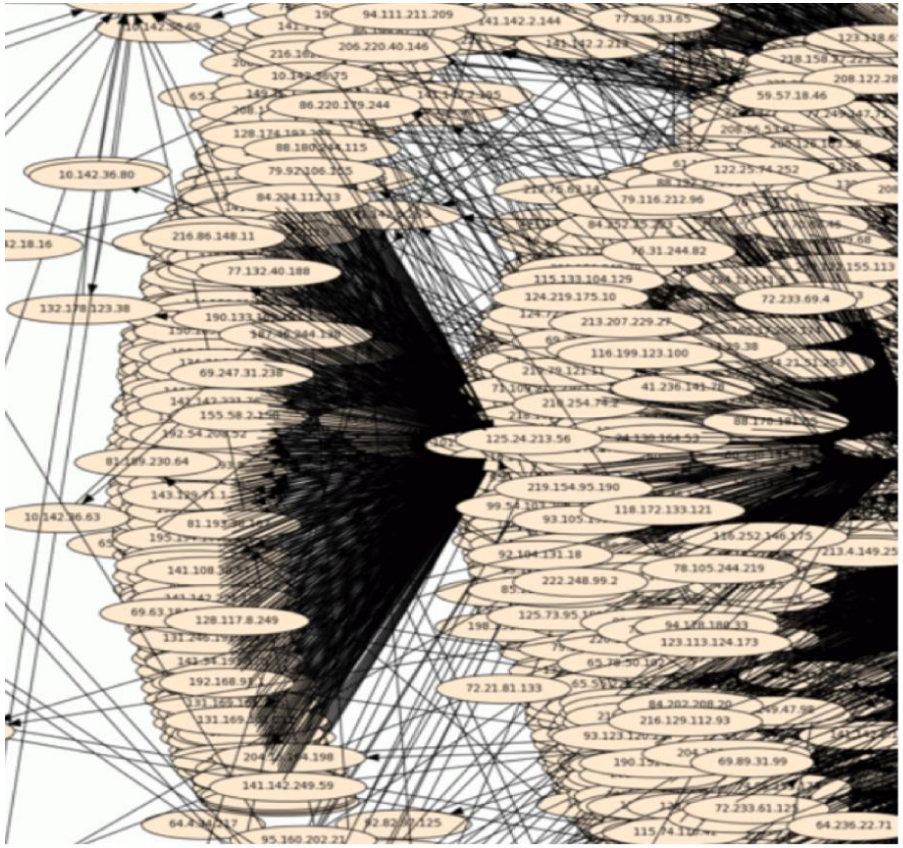
Cloud Computing - Growing Interest vs. Increasing Number of Outages



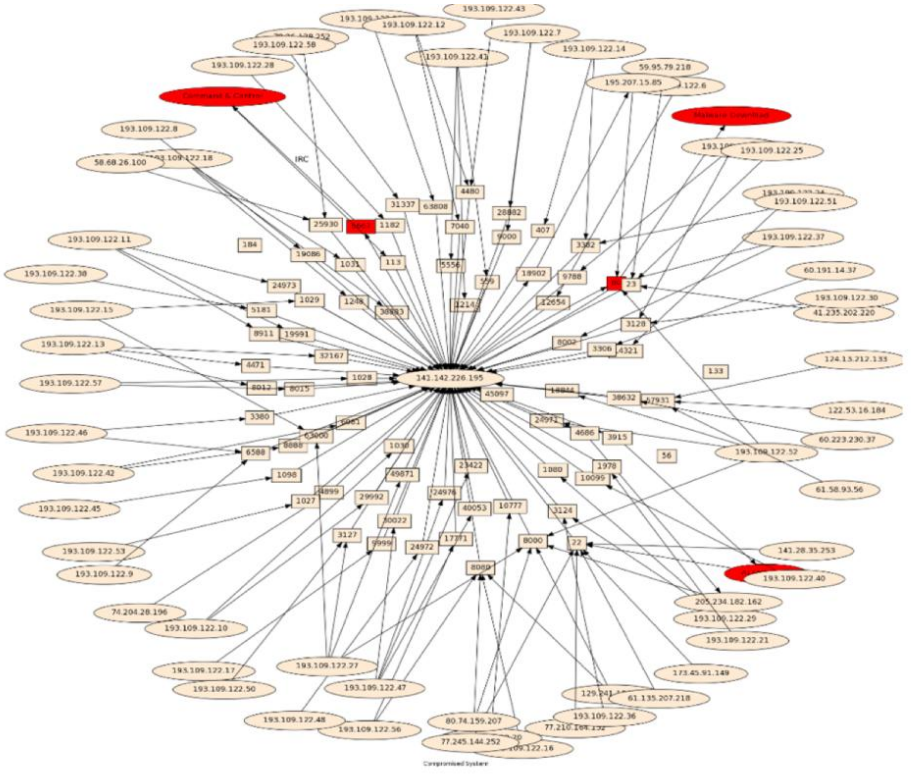
- Providing a higher level of reliability and availability is one of the biggest challenges of Cloud computing

Magnitude of the Problems:

Five-Minute Snapshot of In-and-Out Traffic within NCSA



(a)



(b)

Incidents with Cloud Computing (1)

- **Providers**
  - **“I discovered that several systems on the Amazon EC2 network were preforming brute force attacks, against our VoIP servers.”**

    (http://www.stuartsheldon.org/blog/2010/04/sip-brute-force-attack-originating-from-amazon-ec2-hosts/)
  - **“Complaints of rampant SIP Brute Force Attacks coming from servers with Amazon EC2 IP Addresses cause many admins to simply drop all Amazon EC2 traffic.”**

    (http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/)
  - **No guarantee that providers will financially survive. What will happen if your provider liquidates? “Cassatt, the San Jose, Calif.-based provider of cloud computing environments, has sold its assets to public IT management firm CA for an undisclosed sum. ”**

    (http://venturebeat.com/2009/06/04/cloud-provider-cassatt-sells-out-to-ca-to-avoid-bankruptcy/)
- **Attacks**
  - **BitBucket, DDoS’s Off The Air. “Starting Friday evening, our network storage became virtually unavailable to us, and the site crawled to a halt.”**

    (http://blog.bitbucket.org/2009/10/04/on-our-extended-downtime-amazon-and-whats-coming/)

Incidents with Cloud Computing (2)

- **Maintenance**
  - **Maintenance Induced Cascading Failures. “Gmail's web interface had a widespread outage earlier today, lasting about 100 minutes”**

    (http://gmailblog.blogspot.com/2009/09/more-on-todays-gmail-issue.html)
- **Storage**
  - **T-Mobile: we probably lost all your Sidekick data “Well, this is shaping up to be one of the biggest disasters in the history of cloud computing, and certainly the largest blow to Danger and the Sidekick platform: T-Mobile's now reporting that personal data stored on Sidekicks has "almost certainly has been lost as a result of a server failure at Microsoft/Danger."”**

    (http://www.engadget.com/2009/10/10/t-mobile-we-probably-lost-all-your-sidekick-data)
- **Power**
  - **Lightning Strike Triggers Amazon EC2 Outage “Some customers of Amazon’s EC2 cloud computing service were offline for more than four hours Wednesday night after an electrical storm damaged power equipment at one of the company’s data centers**

    (http://www.datacenterknowledge.com/archives/2009/06/11/lightning-strike-triggers-amazon-ec2-outage/)

Recent Outages

- Amazon Cloud
  - June 2012, Netflix Instagram, Pinterest, Heroku
  - October 22, 2012 takes down Reddit, Airbnb, Flipboard, Coursera
- Storm
  - October 29, 2012 Datagram – Web Hosting- Huffington Post

Verizon, New York
Also Con Ed shut down.

Dependability in Tomorrow's Cloud

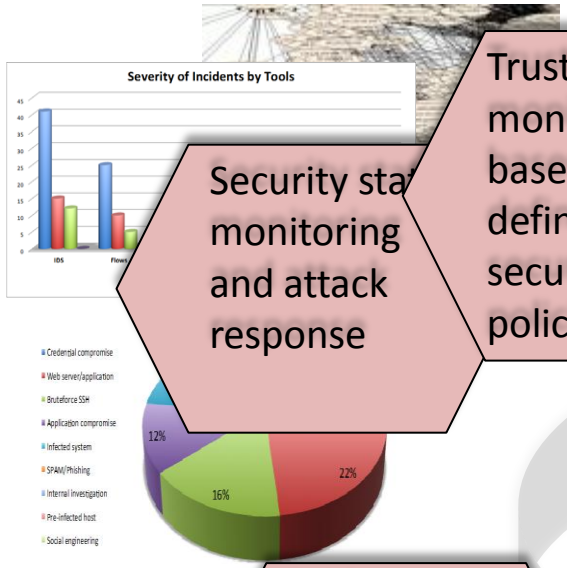
- *Dependability at scale*
  - Think about exabytes systems in the next decades

- How do we make such systems secure?
  - Understand the attacker
  - Monitor and manage huge dynamic systems
  - Create end-to-end security
- How do we make them reliable reliable?
  - Thousands of failures a day could be the norm
  - Hardware changes will require rethinking software

Principles

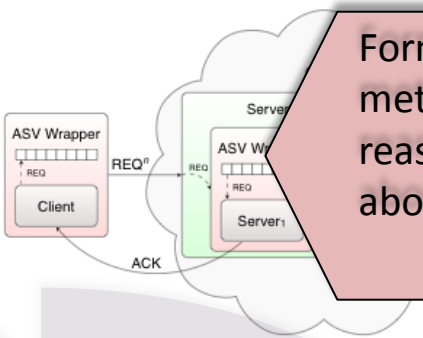
- **Dependability and Security Resilience should scale linearly with Cloud scaling.**
  - Management
    - Virtualization (machines and networks)
    - Authentication / Authorization
  - Monitoring
    - Logging
    - Auditing
  - Encrypted databases
  - Privacy
  - Dependability in Big Data

Towards Assured Clouds: Our Approach

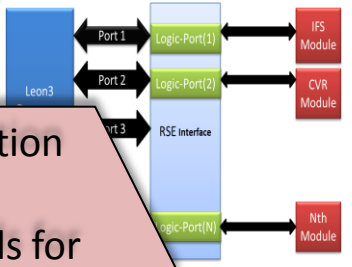


Security sta monitoring and attack response

Trustworthy monitoring based on user-defined security policies



Formal methods and reasoning about cloud

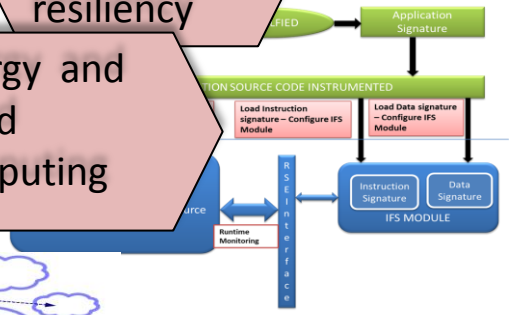


Application aware methods for failure and attack resiliency

Assured Cloud Computing

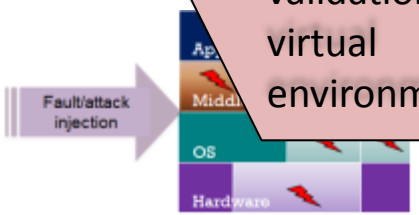
Cost effective

Environment friendly

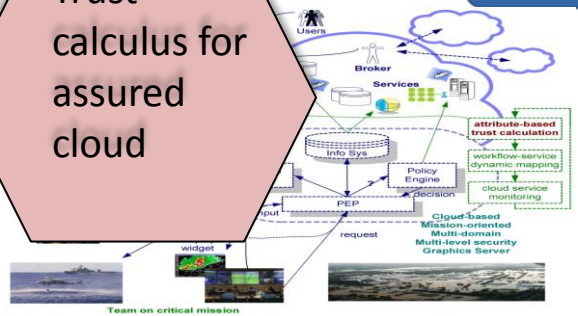


Energy and cloud computing

Evidence-based policy compliance monitoring



Design, verification, and validation of virtual environments



Trust calculus for assured cloud

Outline

- Principles
- **Security at scale** ←
  - Adversary models for cloud computing
  - Management and monitoring
  - End-to-end security in cloud computing
  - Privacy of user and data
  - Delegation and authorization in cloud computing
- Dependability at scale
  - Characterizing failures in big-data systems
  - Managing metadata
  - Cloud, machine learning, and dependability

Securing the Cloud

- **Security** must become a first order design principle:
  - Disruptive technologies such as multi-sensory phones and mobile Internet have a major impact on distributed computing. Mobile clients and their applications want access to data and computation anytime and anywhere. Major industry trends shifting traditional distributed computing to large-scale mega-datacenters

- *Scale changes everything*
  - attestation processes, done very well for current smaller scale systems, will not scale well for large scale open systems.
  - Current trusted platform modules (TPMs) are too passive and might be inadequate for large scale systems.
  - For large scale systems, hierarchical trust will need to be reconsidered (Can we really trust the cloud service provider?).
  - With large scale, nodes will be disposable in clouds, which may disrupt cloud security infrastructure put in place.

Outline

- Principles
- Security at scale
  - **Adversary models for cloud computing ←**
  - Management and monitoring
  - End-to-end security in cloud computing
  - Privacy of user and data
  - Delegation and authorization in cloud computing
- Dependability at scale
  - Characterizing failures in big-data systems
  - Managing metadata
  - Cloud, machine learning, and dependability

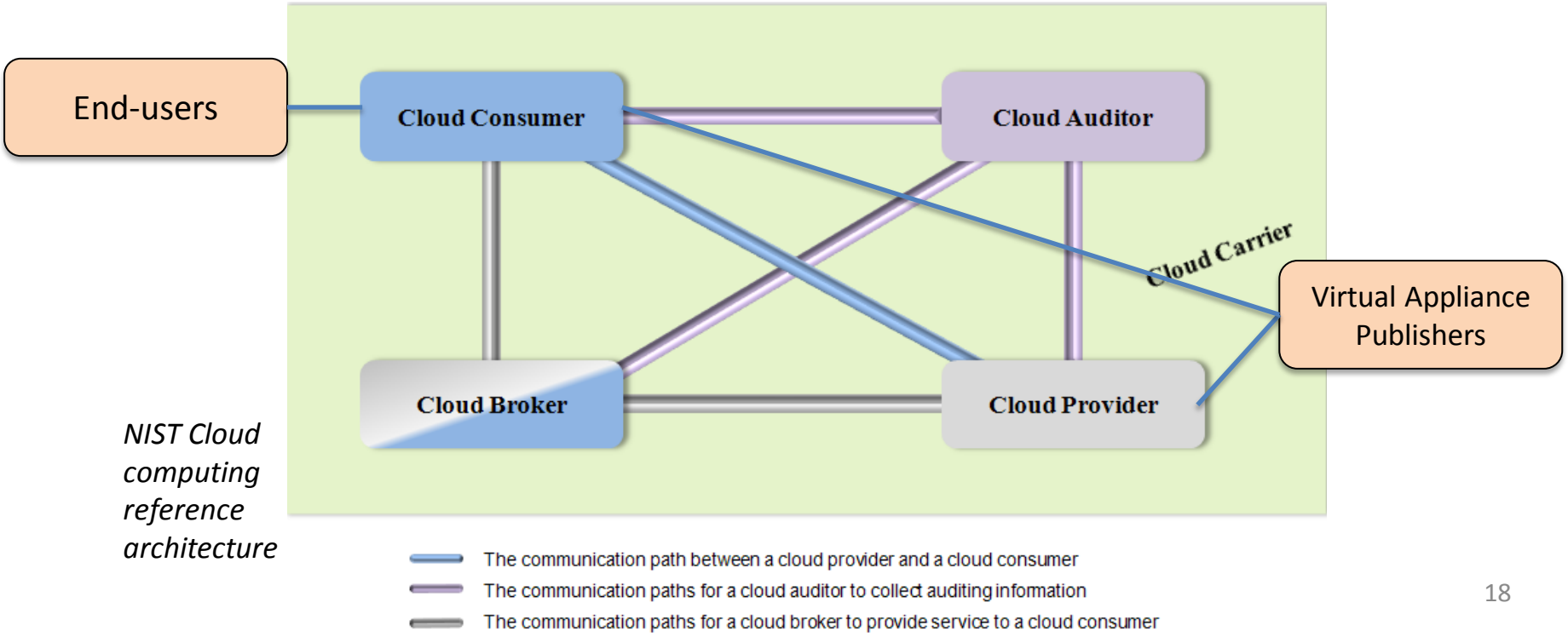
Challenge: Adversary models for cloud computing

What does an adversary look like in cloud computing when different entities are involved such as when a client is a user, an owner, a storage provider and a compute provider and when some or all of the entities in the cloud can become adversaries?

- consider new adversary models for new situations,
- develop techniques to check cloud applications for vulnerabilities, and
- explore protection techniques for data, and enable multi-level security.

Many new players in the Architecture

- New domain of security with many players
  - Many players: cloud consumer; cloud providers; cloud auditors; cloud brokers; cloud carriers; virtual appliance publishers; end-users.
  - What if any is malicious?



NIST Cloud computing reference architecture

Example: Security of Virtual Appliances

- A virtual appliance (VA) is a virtual machine + some combination of software installed, serving a certain purpose
  - E.g. "Java Web Starter" has CentOS, Java, Tomcat, MySQL installed.
- There is no way for a VA consumer to check how *trustable* a VA is
  - Is it configured with all the needed software?
  - Are the needed software installed *properly*?

- For example, we could use a *software whitelist*-based framework for verifying trust levels of VAs
  - Verify every file in a VA against a whitelist of known-good files (comparing their hashes)
  - Based on the *unknown/unverified* files and *missing* files, we generate a verification report that documents
    - List of installed software packages
    - List of unknown files and missing files
    - "Integrity rating" for each software package

Jun Ho Huh, Mirko Montanari, Derek Dagit, Rakesh B. Bobba, Dong Wook Kim, and Roy H Campbell, *"Assessing software integrity of virtual appliances through software whitelists: Is it any good?" NDSS 2013 Short Talk*

Evaluation and Results

- We tested our framework on 151 VAs collected from Amazon, showing
  - High variances in the number of unverified/missing files across those VAs
  - High variances in the number of potentially untrusted software packages
  - 9% of real world VAs have significant numbers of software packages that contain unknown files
  - Virus scanners detected only half of the VAs in that 9% as potentially malicious
- High variances in the number of untrusted packages across the VAs demonstrate the *usefulness* of the framework

Outline

- Principles
- Security at scale
  - Adversary models for cloud computing
  - **Management and monitoring ←**
  - End-to-end security in cloud computing
  - Privacy of user and data
  - Delegation and authorization in cloud computing
- Dependability at scale
  - Characterizing failures in big-data systems
  - Managing metadata
  - Cloud, machine learning, and dependability

Challenge: Management and Monitoring

- How do we manage the large datacenters?
  - Virtual machine security and management
  - Virtual networks
    - Software Defined Networks: e.g. Openflow (E.g. central or hierarchical managed connectivity)
- How do we ensure that a cloud system is "working correctly"?

Manage the Complexity: Policies

How do we know if the system we are monitoring is operating correctly?

cloud computing systems	*virtualized systems*	*multi-organization systems*

- A **policy-based approach** helps manage the complexity of the system

Examples of policies from Payment Card Industry Data Security Standard (PCI-DSS)

"1.3) Prohibit direct public access between the Internet and any system component in the cardholder data environment."

"6.1) Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release."

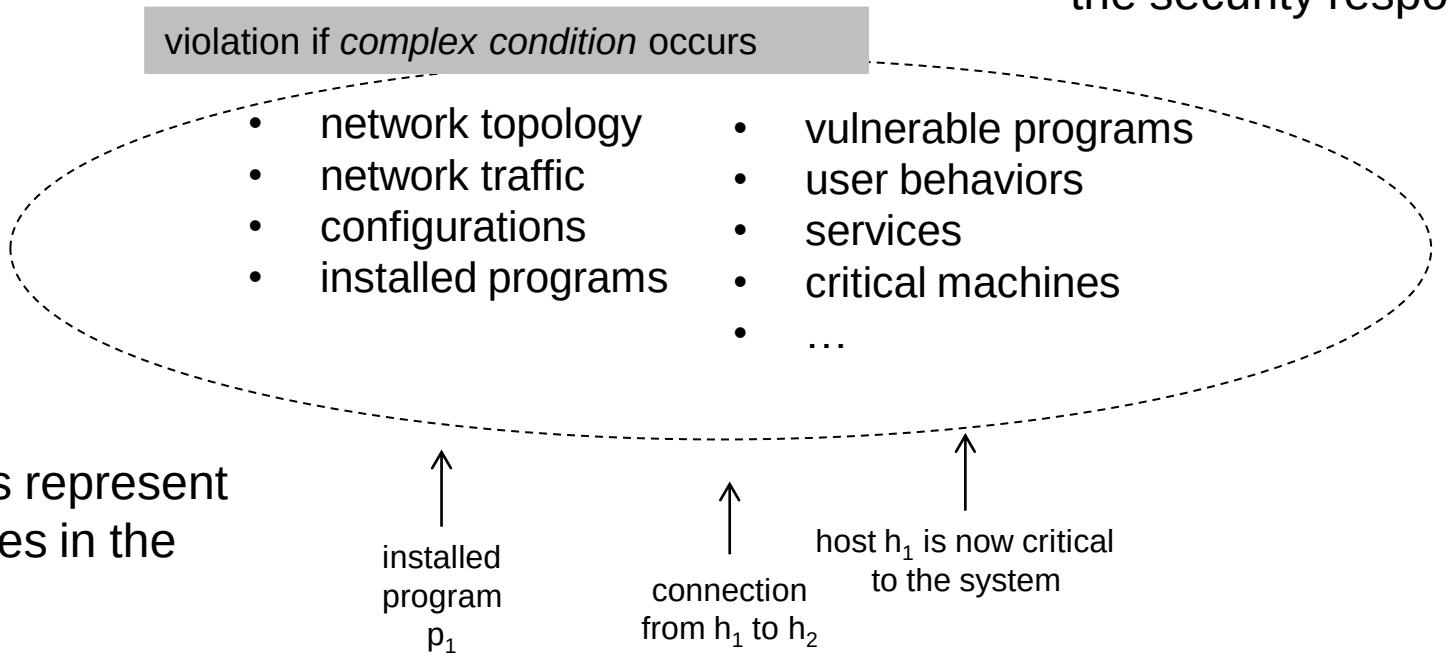
Mirko Montanari, Roy H. Campbell, "Confidentiality of Event Data in Policy-Based Monitoring," DSN 2012

Event Correlation

- Network administrators can use security monitoring to ensure that the system is operating according to the policies
  - Event correlation: process of analyzing events for detecting complex conditions

Policy violations are conditions identifying incorrect behaviors of the system

Information about policy violations drives the security responses



Security Challenges for Monitoring

- A large part of security management is based on monitoring

How do we secure the event-correlation process?

Monitoring systems need to operate in challenging conditions:

software and hardware vulnerabilities *0-day attacks*

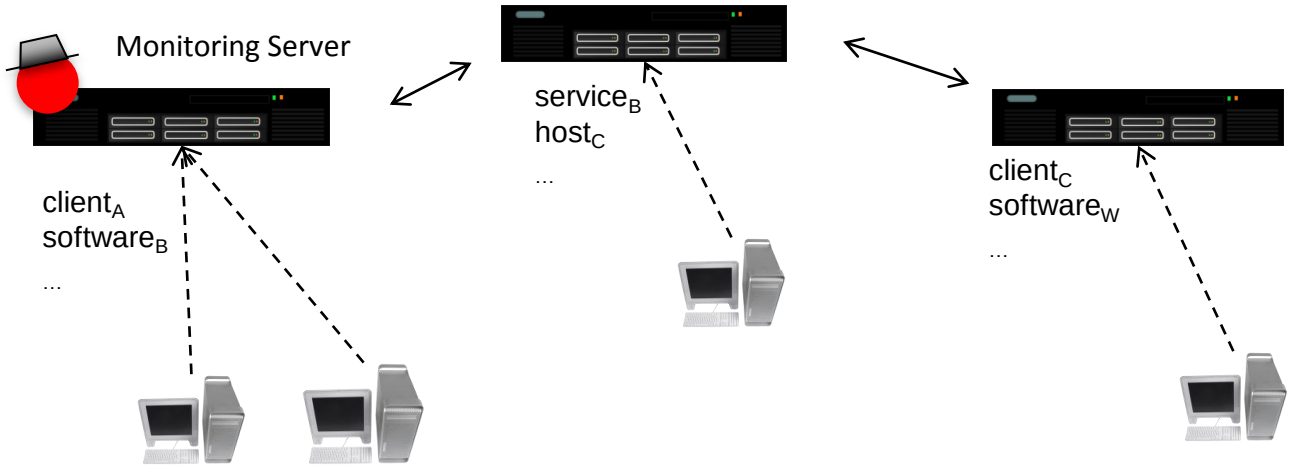
virtualized environments *systems spanning across multiple security domai*

How do we create monitoring systems that can survive complex attacks?

How do we create monitoring systems for tightly coupled multi-domain systems?

Intrusion-tolerant Event Correlation

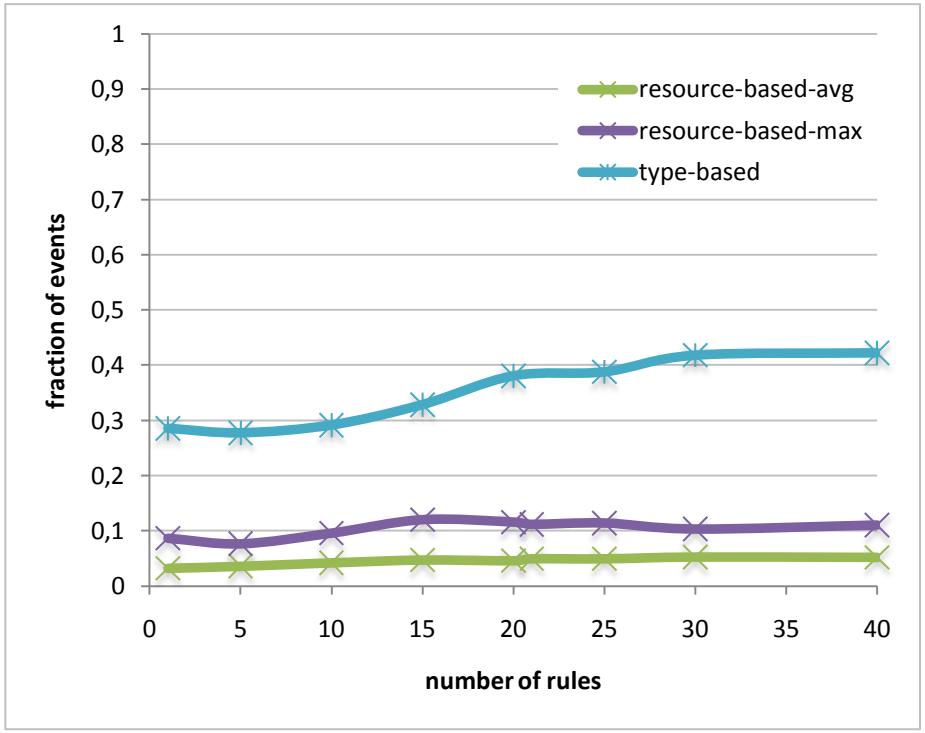
- Force malicious users to collect more credentials or compromise more machines to collect information
- *Take advantage of the structure of organizations*: monitoring servers managed by different units are in different networks and use different credentials
- Each monitoring server receives events about a limited number of resources in the system



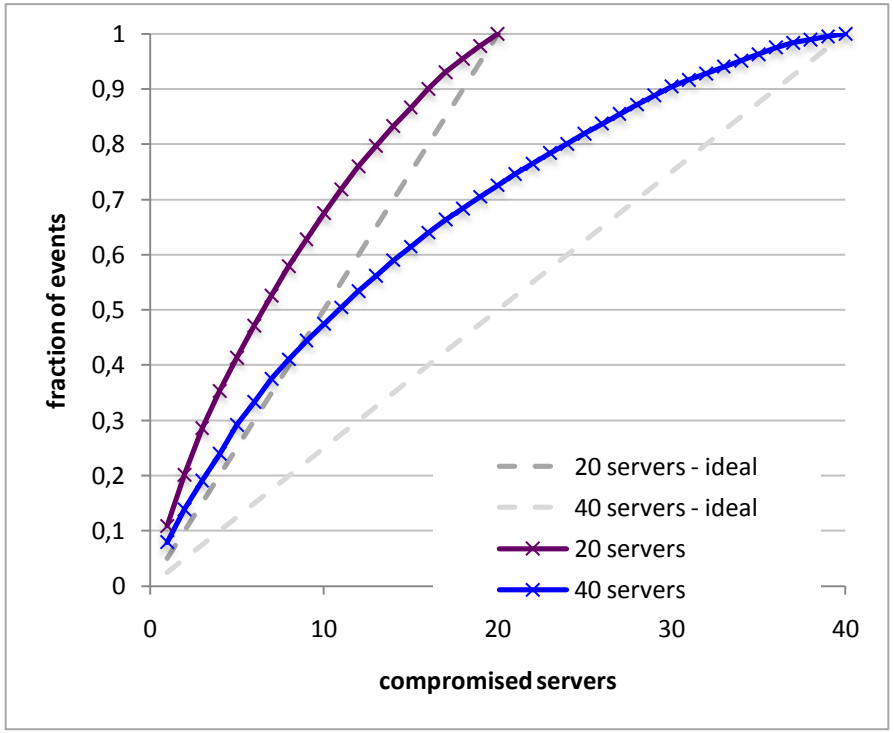
- The compromise of a monitoring server only reveals limited information

Scaling of Information Exposure

Measure the capacity of our solution to limit exposure of information and distribute load



Events in one monitoring server



Compromise of multiple monitoring server

- EC2 deployment of the monitoring system (40 servers)
- Event traces generated through a probabilistic model created by collecting events from 5 shared lab machines and servers, and by scaling up the dataset.

Outline

- Principles
- Security at scale
  - Adversary models for cloud computing
  - Management and monitoring
  - **End-to-end security in cloud computing ←**
  - Privacy of user and data
  - Delegation and authorization in cloud computing
- Dependability at scale
  - Characterizing failures in big-data systems
  - Managing metadata
  - Cloud, machine learning, and dependability

End-to-end security in cloud computing

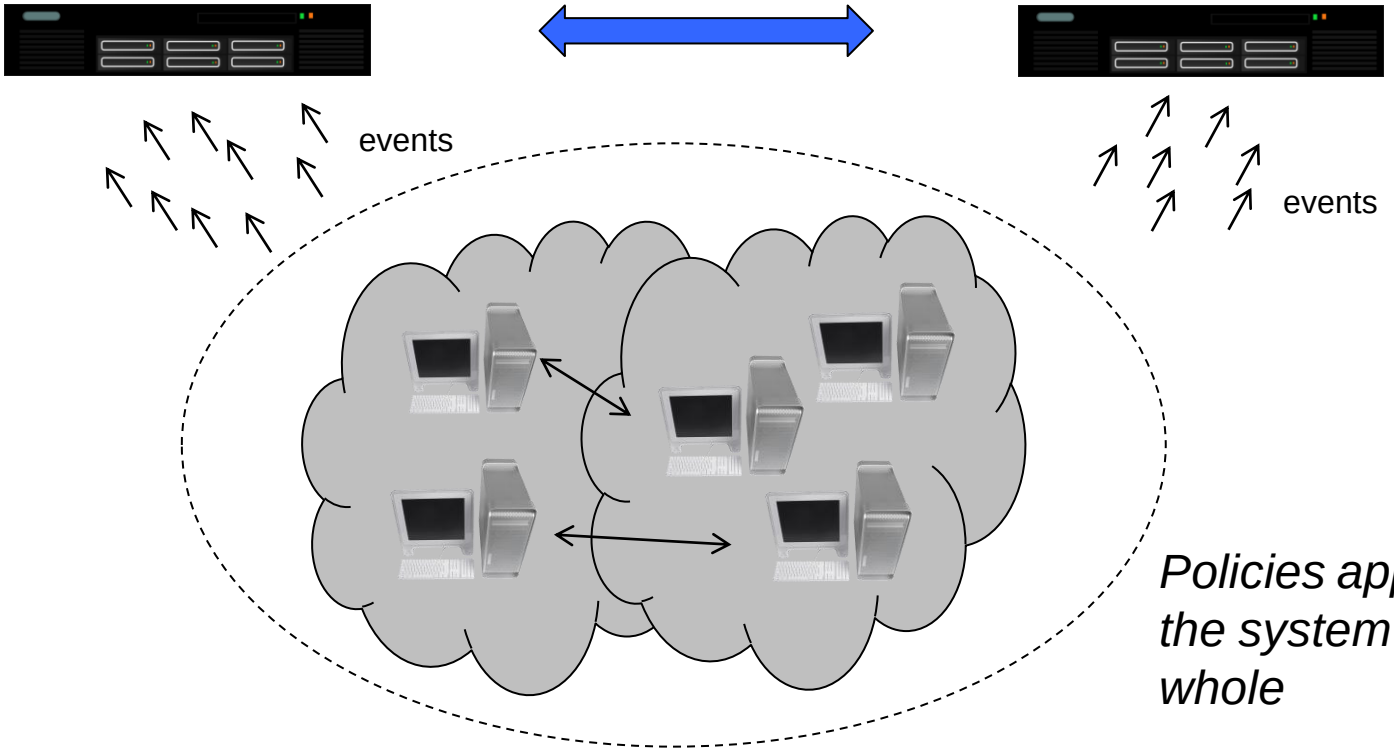
Cloud computing is not an isolated entity in the computing ecosystem but it is always connected with a client(s) who wants certain work (storage, computation, response) from the cloud service.

- investigate systematically tradeoffs between security and efficiency at each component (clients, networks and clouds) of the end-to-end problem,
- consider approaches towards securing data and applications on secure client devices against untrusted cloud platforms,
- explore platforms for private data,
- investigate policy-based security applied to end-to-end cloud computing.

Multi-Domain Monitoring

- Systems composed of multiple security domains are common
  - E.g., airport systems, cloud computing systems, large organizations

- Different monitoring systems manage the different parts of the infrastructure
- Monitoring data is integrated to detect attacks, or to find problems that span multiple systems (e.g., sharing audit logs in cloud computing environment)



Mirko Montanari, Lucas T. Cook, Roy H. Campbell, "Multi-organization policy-based monitoring, " POLICY 2012

Information Sharing Strategies

- Can we decide which events to share without having complete knowledge of the state of the other organization?

The explicit definitions of policies reduces the information to share:

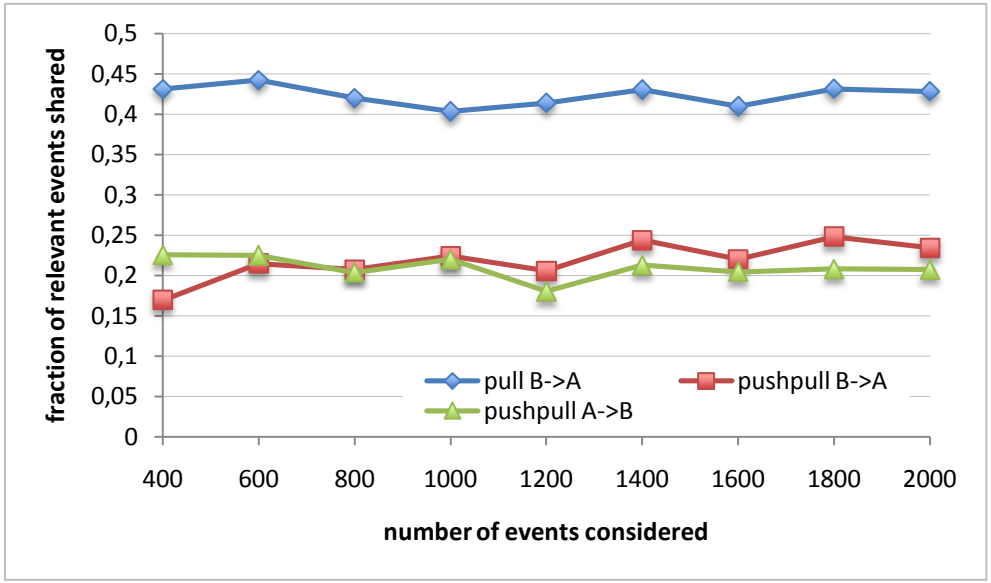
Pull strategy: one organization is willing to reveal events unconditionally (e.g., a subordinate organization)

Locality information to reduce the amount of events to share

Push-pull strategy: organizations are both reticent in sharing information

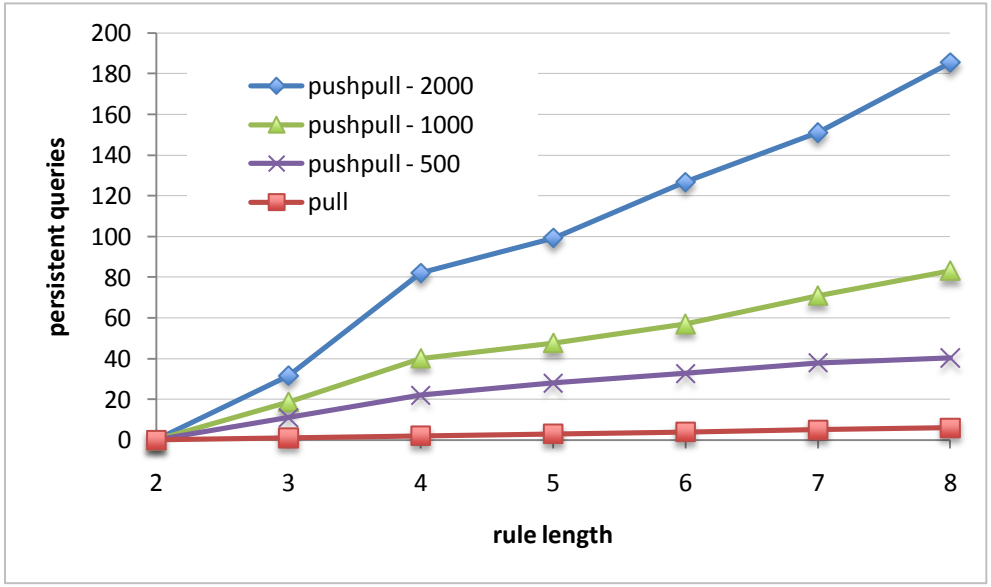
One organization shares some information about its state to better identify the events that can cause a violation

Reduced Events to Share



Fraction of events shared

Only 20% of the relevant events need to be shared by each organization



Load on the system

- Number of persistent queries submitted

Push-pull load grows with the number of current events and the rule length

Outline

- Principles
- Security at scale
  - Adversary models for cloud computing
  - Management and monitoring
  - End-to-end security in cloud computing
  - **Privacy of user and data ←**
  - Delegation and authorization in cloud computing
- Dependability at scale
  - Characterizing failures in big-data systems
  - Managing metadata
  - Cloud, machine learning, and dependability

Privacy in Cloud Computing

- Protecting the privacy of organizations using the cloud from the cloud provider
  - Virtualization solution / access control
  - Encryption

- Protecting the privacy of user data in the cloud where infrastructure might span multiple political boundaries

Privacy Research Findings

The location of a cloud provider's data center greatly affects the way in which users are legally protected because individual jurisdictions vary in terms of cloud policy and regulation.

- In the U.S., data centers are subject to the USA PATRIOT Act, the Homeland Security Act, and National Security Letters.
- To avoid the reach of these laws, providers have begun construction of data centers in neutral areas
  - An international banking organization, known as SWIFT, is considering a neutral country (Switzerland) as its data center, in an attempt to avoid legal complications and risks.

- Recently, the European Union passed an ePrivacy Directive that requires a user's consent before a provider begins to store and access information.

- It also places limits on the transfer of personal data by companies to foreign countries, requiring those countries to offer adequate protection for the privacy of the information.
  - The United States does not provide adequate privacy protections under EU standards, but many companies in the U.S. obtain a **Safe Harbor certification** that permits them to transfer personal information from the European Union to the United States.

Privacy -Future Directions

- Analyze a larger sample size of privacy policies and terms of service
- Examine implications of requiring greater privacy protections, especially on companies that provide cheap or free services supported by advertising revenue:
  - Is the devaluing of privacy online actually a problem?
  - If a baseline of privacy protections is required, would that require some companies to: (1) Decrease sale of advertising, and/or (2) Start charging for formerly free services?
  - Evaluate the normative questions related to whether people should have the option to trade their privacy rights for free, convenient services
- 4th Amendment issues:
  - Does the third party doctrine limit or prevent 4th amendment protection of information online, due to the need for third parties to process such information?
  - To the extent that a "Reasonable Expectation of Privacy" (REOP) relies on society's view that the expectation is reasonable, might a societal devaluing of privacy online lead to a finding that there is no REOP in virtually anything on the web?
- Stored Communications Act: Might consenting to excessively broad privacy policies amount to a consent to disclosure of information stored in the cloud under the SCA?
- What effect does the FTC's enforcement of privacy policies have on what a company puts in their privacy policy? Might this explain why companies tend to be more vague when the policy provisions concern the customer's rights?

Outline

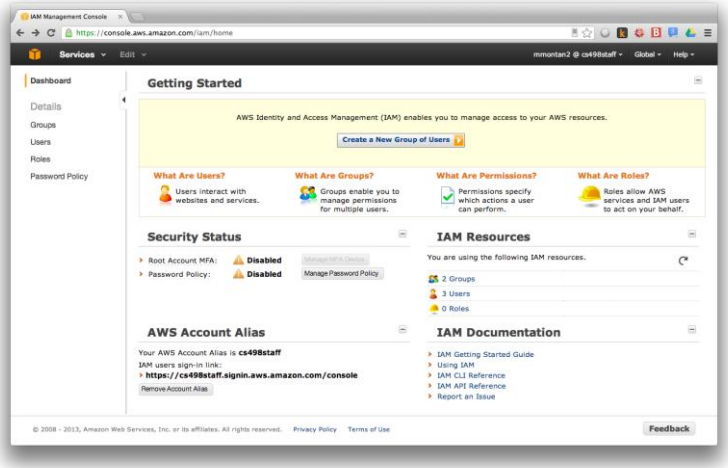
- Principles
- Security at scale
  - Adversary models for cloud computing
  - Management and monitoring
  - End-to-end security in cloud computing
  - Privacy of user and data
  - **Delegation and authorization in cloud computing ←**
- Dependability at scale
  - Characterizing failures in big-data systems
  - Managing metadata
  - Cloud, machine learning, and dependability

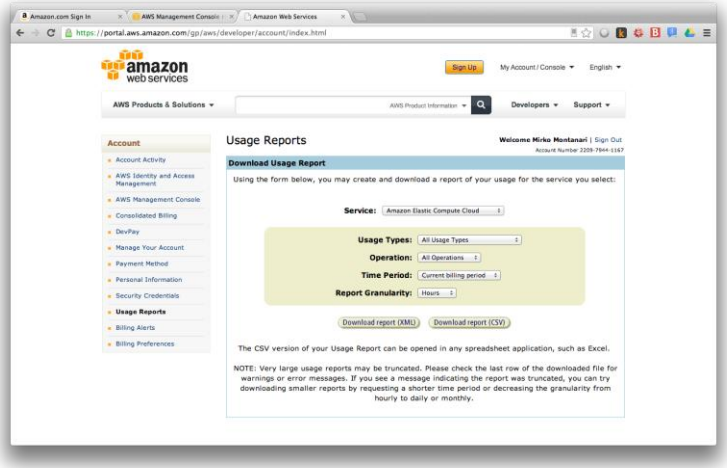
Delegation and authorization in cloud computing

With cloud computing, we will see more and more third parties accessing clouds on behalf of users.

- investigate efficient encryption and decryption delegation mechanisms,
- explore extensively computation over encrypted and authenticated data,
- research secure comparison mechanisms, access control with capabilities, and delegation and authorization challenges in scientific clouds.

Examples





- Amazon AWS role based management and auditing
- How do we extend tools to federated cloud systems and cloud brokers in a scalable way?

Outline

- Principles
- Security at scale
  - Adversary models for cloud computing
  - Management and monitoring
  - End-to-end security in cloud computing
  - Delegation and authorization in cloud computing
  - Privacy of user and data
- **Reliability at scale ←**
  - Characterizing failures in big-data systems
  - Managing metadata
  - Cloud, machine learning, and dependability

Reliability at Scale

- Does BIG DATA have any characteristics that can be used to improve availability, security and reliability?
  - Understanding the impact of failures in Big Data applications
  - Evaluating the implication of metadata in large clusters

Outline

- Principles
- Security at scale
  - Adversary models for cloud computing
  - Management and monitoring
  - End-to-end security in cloud computing
  - Delegation and authorization in cloud computing
  - Privacy of user and data
- Reliability at scale
  - **Characterizing failures in big-data systems ←**
  - Managing metadata
  - Cloud, machine learning, and dependability

How do we deal with failures?

- We spend more $$$ for Premium hardware
  - high costs
- We use small sandbox-testing models
  - not sufficient to predict production-level failures

OR

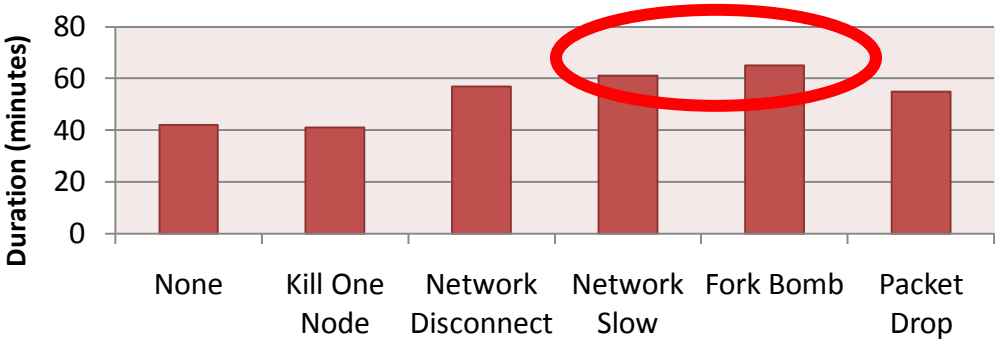
- We inject failures!
  - Chaos Monkey by NETFLIX
  - Anarchy Ape by YAHOO!

Faraz Faghri, Sobir Bazarbayev, Mark Overholt, Reza Farivar, Roy Campbell and William Sanders, "Failure Scenario as a Service for Hadoop Clusters," Secure and Dependable Middleware for Cloud Monitoring and Management, 2012

Failure Injection to Create Models

- We inject failures, But good failure injection requires many diverse failure scenarios.
  - we select most impactful failures for different applications.

- But there are so many applications!
  - Therefore we classify Hadoop-type applications based on workloads and inject selected most impactful failures:
    - I/O intensive workload (e.g. *random writer*)
    - CPU intensive workloads (e.g. *word count)*
    - Network intensive workloads (e.g. *text sort)*

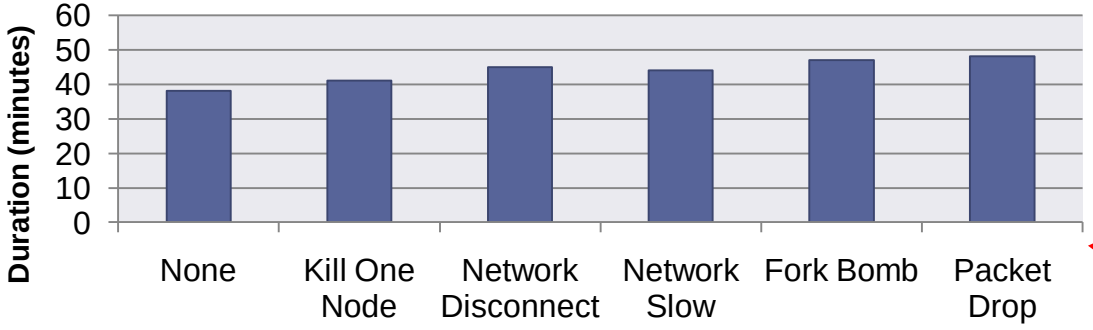


Failures on Word Count (CPU intensive)

Processor related failures are more impactful

Failures on Sort (Network intensive)

Network related failures are more impactful



Failures on Random Writer (I/O intensive)

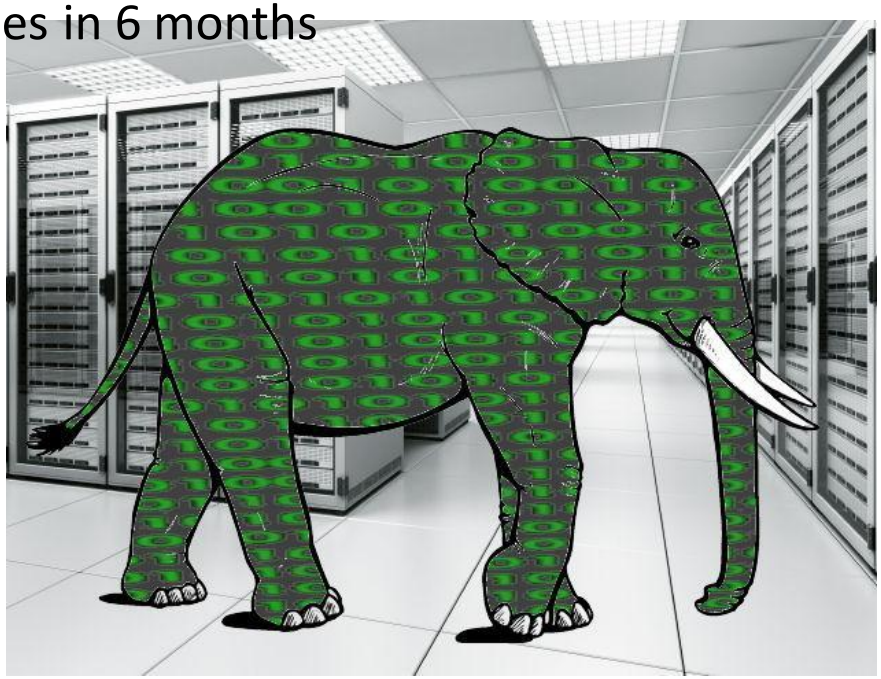
non I/O related failures at same level of impact

Outline

- Principles
- Security at scale
  - Adversary models for cloud computing
  - Management and monitoring
  - End-to-end security in cloud computing
  - Delegation and authorization in cloud computing
  - Privacy of user and data
- Reliability at scale
  - Characterizing failures in big-data systems
  - **Managing metadata ←**
  - Cloud, machine learning, and dependability

Cloud Storage Workload Characterization and Modeling

- Dependability of metadata necessary for large systems
- Studied how MapReduce interacts with storage layer [1]
- Findings relevant to storage system design and tuning:
  - Workloads are dominated by high file churn
  - 80%–90% files accessed 1-10 times in 6 months
  - Small % of very popular files
  - Young files:
    - High % of accesses,
    - Small % of bytes stored
  - Requests are bursty
  - Files are very short-lived:
    - 90% deletions target files < 1.25 hours old



[1] Abad, C., Roberts, N., Lu, Y., and Campbell, R.. "A Storage-Centric Analysis of MapReduce Workloads: File Popularity, Temporal Locality and Arrival Patterns". (to appear in) Proc. IEEE International Symposium on Workload Characterization (IISWC), 2012.

Cloud Storage, Big Data, Design Implications

- Design/tuning of storage systems:
  - Improved performance and scalability
- Implications of observed behavior:
  - The peculiarities observed are mostly derived from short-lived files and high file churn
    - File churn is a result of typical MapReduce workflows
  - Must research on appropriate storage media and tiered storage approaches
  - Caching young files or placing them on a fast storage tier would lead to performance improvement at a low cost
  - *Inactive storage* constitutes high % of stored bytes and files
    - Timely file recovery and choice of replication scheme and media for passive data needed for improved utilization
  - A model of file popularity must consider a very dynamic population

Big Data Storage Workloads: Modeling and Synthetic Generation

- One potential storage bottleneck:
  - Metadata server: must handle large number of bursty requests
- New schemes have been proposed but evaluation has been insufficient
  - No adequate traces or models
- Mimesis [2]: synthetic workload generator
  - Suitable for Big Data workloads
  - Reproduces desired statistical workload of original trace
  - Accurate: low RMSE (root mean squared error) when used in place of original traces
    - Used to evaluate a LRU metadata cache for HDFS

[2] Abad, C., Luu, H., Roberts, N., Lee, K., Lu, Y., and Campbell, R.. "Metadata traces and workload models for evaluating Big storage systems," (to appear in) Proc. IEEE/ACM Int'l Conf. Utility and Cloud Comp. (UCC), 2012.

Outline

- Principles
- Security at scale
  - Adversary models for cloud computing
  - Management and monitoring
  - End-to-end security in cloud computing
  - Delegation and authorization in cloud computing
  - Privacy of user and data
- Reliability at scale
  - Characterizing failures in big-data systems
  - Managing metadata
  - **Cloud, machine learning, and dependability ←**

Clouds, Machine Learning and Reliability

- Trend: Clouds will expand into diverse roles
  - Big Data → Data mining and machine learning
  - Real time data → Streaming clouds (e.g. Storm)
  - Economic pressure: Massive clouds adoption
  - Results fed into Cyber physical systems
- Result: The reliability and security of (1) clouds and (2) ML algorithms on clouds will impact real-world phenomena
- The current cloud solutions are orders of magnitude less dependable than minimum requirements for cyber physical systems

Security of Machine Learning

- Influence
  - Causative attacks influence learning with control over training data
  - Exploratory attacks exploit misclassifications but do not effect training
- Security Violations
  - Integrity attacks compromise assets via false negatives
  - Availability attacks cause denial of service, usually via false positives
- Specificity
  - Targeted attacks focus on a particular instance
  - Indiscriminate attacks encompass a wide class of instances

Barreno, Marco; Nelson, Blaine; Joseph, Anthony, Tygar, J.; The security of machine learning, Machine Learning (2010) 81: 121-148.

Conclusion

- Dependability in Tomorrow's cloud is a dependability at scale
- Challenges in security and reliability given by the new conditions and the scale
  - New attack models and reliability models; scalable and security management and monitoring; privacy; metadata management.

- Lots of work still need to be done

References

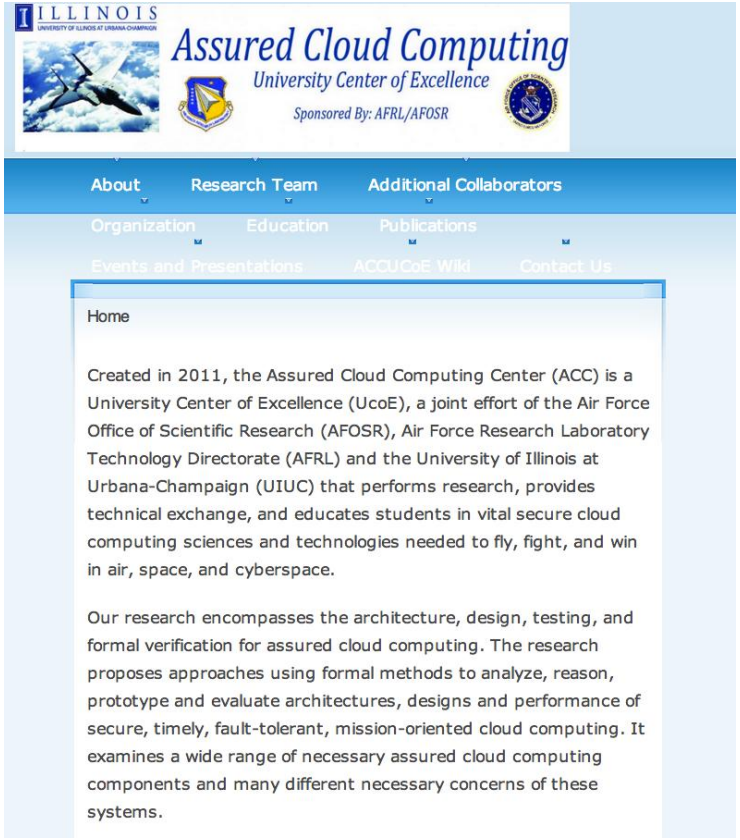
Report to the National Science Foundation
Directorate for Computer and Information Science and Engineering (CISE)

Security for Cloud Computing

Klara Nahrstedt and Roy Campbell
University of Illinois at Urbana-Champaign

March 15-16, 2012
Arlington, Virginia

http://illinois.edu/blog/view/695/66281?count=1&ACTION=DIALOG



https://illinois.edu/blog/dialogFileSec/2737.pdf http://assured-cloud-computing.illinois.edu/

Questions?
Thanks

Roy Campbell
rhc@illinois.edu

New problems in security for cloud computing

- investigate hardware and software virtualization architectures that would enable security and performance isolation at all levels;
- explore dynamic platforms, dynamic verifications, dynamic attestation techniques, fine-grain logging for user-driven secure auditing;
- research customizable new security mechanisms, security of public clouds, security risks coming from side channels, reactive stability, and other risks we are not looking at yet or not carefully enough;
- investigate in an inter-disciplinary fashion cloud forensics;
- explore alternative solutions to securing the cloud, such as cheap and automated system operations for users.